

The Akenti Access Control System: Resource Access Control with Authorization and Attribute Certificates¹

(An Application of Public-key Infrastructure and Digitally Signed Certificates)

William E. Johnston², Srilekha Mudumbai, Mary Thompson, Gary Hoo, and Keith Jackson
Information and Computing Sciences Division
Ernest Orlando Lawrence Berkeley National Laboratory
University of California



1. This work is supported by the Director, Office of Energy Research, Office of Computation and Technology Research, Mathematical, Information, and Computational Sciences Division, of the U. S. Department of Energy under Contract No. DE-AC03-76SF00098 with the University of California. See <http://www-itg.lbl.gov/Security/Akenti> for more information.
2. wejohnston@lbl.gov (510-486-5014), mudumbai@george.lbl.gov, mrt@george.lbl.gov - <http://www-itg.lbl.gov>

Imaging and Distributed Computing Group,
Information and Computing Sciences Division

1

[Global.Capability.Akenti.summary.VG.fm - July 22, 1998]



Akenti Access Control System

Security for Widely Distributed Systems

Motivation:

Our scientific environment involves

- multi-user instruments at national facilities
- widely distributed supercomputers and large-scale storage systems
- data sharing in restricted collaborations
- network-based multimedia collaboration channels

and these facilities, collaborations, and stakeholders are diffuse - geographically distributed and multi-organizational.

These circumstances require

- distributed management - because the principals and resources are dispersed organizationally
- distributed access control - because the resources and users are dispersed geographically

Imaging and Distributed Computing Group,
Information and Computing Sciences Division

2

[Global.Capability.Akenti.summary.VG.fm - July 22, 1998]



Akenti Access Control System

Outline

- ◆ Use a Well Understood Approach as a Model
- ◆ Overall Goals
- ◆ Background and Framework
- ◆ General Approach
- ◆ Implementation and Deployment Strategy
- ◆ The General Security Model for Access Control
- ◆ Policy Model
- ◆ Operation of the Akenti Access Control System
- ◆ Authorization Certificates for Apache
- ◆ Authorization Certificates for GSS-API
- ◆ Authorization Certificates for CORBA
- ◆ Certificate Infrastructure
- ◆ User Interaction
- ◆ Identity Establishment
- ◆ Use-conditions
- ◆ Attributes
- ◆ CDS: A Simple Akenti Application
- ◆ Bandwidth Reservation
- ◆ Monitoring



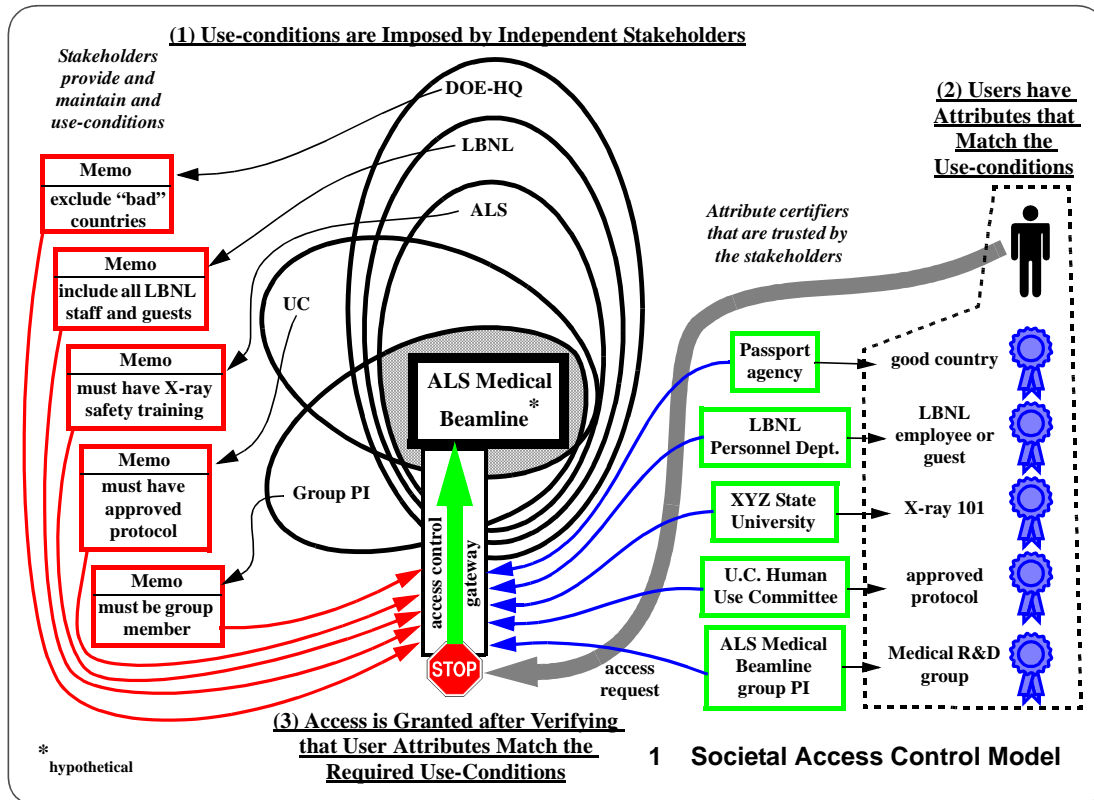
Akenti Access Control System: Model

Use a Well Understood Approach as a Model

- ◆ Stakeholders are identified by (usually) written policy
- ◆ Representations of authority (“use-conditions”) are made by written, signed procedures, memoranda, etc.
- ◆ The required use-conditions are satisfied by a set of attributes: organizational membership, training, etc.
- ◆ Who and/or what can attest to users’ satisfaction of the use-conditions is established by policy: e.g. a token issued by a personnel department, a certificate of training issued by an accredited school, etc.
- ◆ Credential checking is usually based on an operational authority that compiles a list of stakeholder use-conditions and then validates the users’ attributes against this list



Akenti Access Control System: Model



Imaging and Distributed Computing Group,
Information and Computing Sciences Division

5

[Global.Capability.Akenti.summary.VG.fm - July 22, 1998]



Akenti Access Control System: Model

- ◆ All of the attributes that match use-conditions are likely to be packaged into a “capability” - a single document (e.g. a “license” or badge) that names the user, and perhaps the resource and the range of permitted actions
- ◆ The access control enforcer - a door guard, the experiment PI, etc. - typically just validates the capability (e.g., checks the license) when access is requested

This general societal model provides us with the framework for an on-line architecture that accomplishes the same sort of access control for on-line resources.

Imaging and Distributed Computing Group,
Information and Computing Sciences Division

6

[Global.Capability.Akenti.summary.VG.fm - July 22, 1998]



Akenti Access Control System

Overall Goals

On-line access control for the scientific environment must provide:

- ◆ **Secure sharing of resources in a way the reflects currently accepted practice and principles:**
 - **stakeholders independently make assertions about resource use**
 - **trusted third-parties certify user attributes required for the use-conditions**
 - **authenticated users that posses the required attributes easily gain access**
 - **the level of credential checking (and security) is determined by the nature of the resource being protected**



Akenti Access Control System: Goals

- ◆ **Dynamic and easily used mechanisms for generation, maintenance, and distribution of the access control information**
 - **those that make assertions (e.g. establish the use-conditions or attest to user attributes) must be able to do so within their own working environment (usability!)**
- ◆ **Strong assurances that use-conditions are met**
 - **access decisions must be made based on assured information and then enforced by strong security services**
- ◆ **Provide a mechanism to separate access policies from identity policies**
 - **akin to authorization certificates (e.g. X9.45)**



Akenti Access Control System

Background and Framework

- ◆ **Digitally signed documents (an application of public-key cryptography) can provide**
 - **assured assertions (e.g. enumeration of resource use-conditions), and**
 - **user information (name and attributes)****without requiring the physical presence of the signer/certifier (in the same way that we accept holographically signed documents today).**
- ◆ **Certification Authorities provide policy-based identity assurances in the form of widely distributed, digitally signed certificates that bind an identity to a public key (analogous, e.g., to a state issued driver's license) - one type of "signing authority"**



Akenti Access Control System: Background

- ◆ **Other signing authorities are the stakeholders that generate, sign, and distribute their assertions as certificates**
- ◆ **A policy engine and access control gateway identifies stakeholder imposed use-conditions and whether a potential user has met these use-conditions and makes access decision for, e.g., information systems, instruments, communications channels, computing and storage capacity**
- ◆ **Application-level security services that provide secure (confidential and reliable) end-to-end communication enforce access control decisions (e.g. SSL - the Secure Sockets Layer, and GSS - the IETF's General Security Services API)**
- ◆ **Web browsers (e.g. Netscape) and servers (e.g. Apache), and commercial Certification Authorities and directory servers, can provide a general infrastructure for managing certificates.**



Akenti Access Control System

General Approach

- ◆ **Use-condition / authorization certificates**: allow stakeholders to impose their requirements in a “natural and convenient” way - by representing them as digitally signed documents that are generated, maintained, and distributed in the stakeholder’s “local” (working) environment.
- ◆ **Attribute certificates**: attribute certifiers (“verifiers”) provide user characteristics that match use-conditions, again in a natural and convenient way.
- ◆ **Identity**: standard X.509 certificates and Certification Authority infrastructure are used for identifying and authenticating various entities.



Akenti Access Control System: Approach

- ◆ **“Akenti” policy engine**: An independent software module that makes access decisions by
 - identifying all stakeholders’ use-conditions associated with a resource,
 - searching for the corresponding user attributes, and
 - verifying that a potential user matches all stakeholder’s use-conditions.
- ◆ **Capabilities**: For a given resource, Akenti provides a verified user identity, an assured access control decision, and a list of permitted actions. The application (or its agent) then uses these to control specific user actions and to set up a secure communication channel between the user/client and resource.



Akenti Access Control System

Implementation and Deployment Strategy

- ◆ Use as much existing and emerging technology as possible:
 - identity certificate generation and management is provided by Netscape Navigator (v4, and later), the Netscape, or comparable, CA and LDAP directory servers
 - security services are provided by SSL and GSS (for providing secure communication channels)
- ◆ The Akenti policy engine is being kept independent of the application and the security services.
- ◆ The Apache Web server is used as a prototype access control gateway for data and other services that can be invoked with cgi-bin scripts. The standard Apache access control module (*.htaccess*, etc.) is replaced by Akenti.

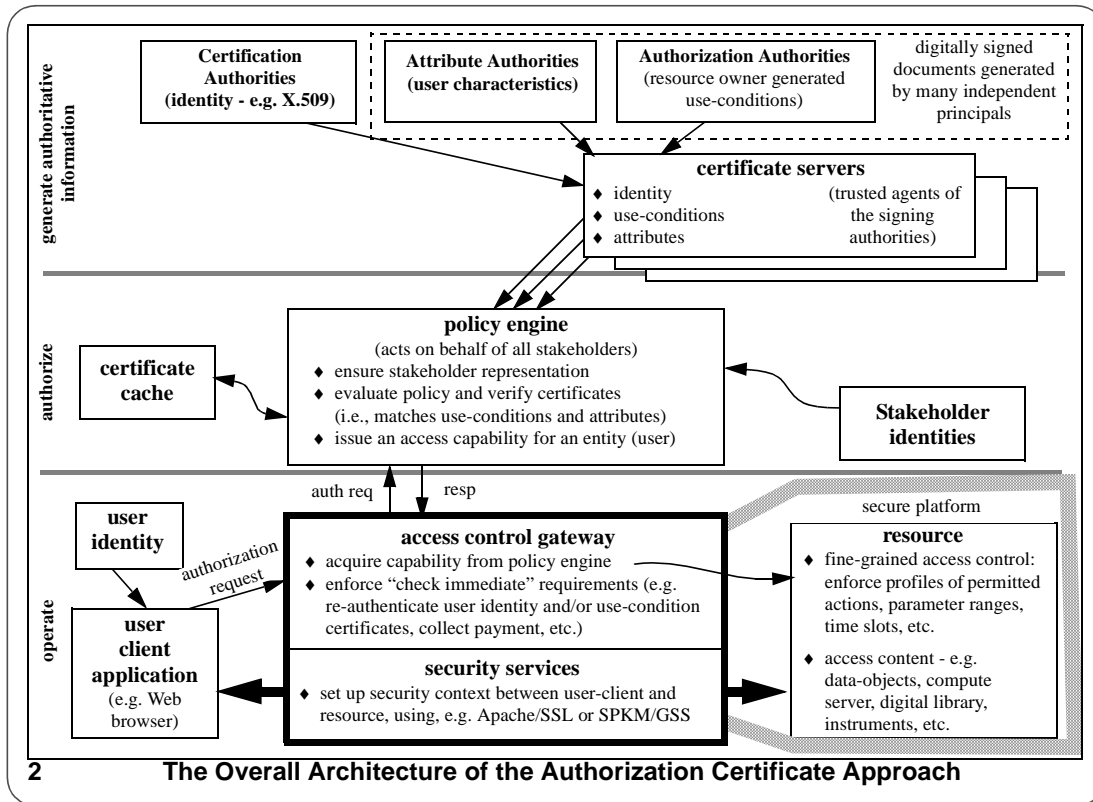


Akenti Access Control System: Implementation

- ◆ Java applications provide the mechanism for stakeholders and attribute certifiers to construct use-condition and attribute certificates.
- ◆ Any Web server “trusted” by the stakeholders and certifiers can be used to distribute the use-condition and attribute certificates.
- ◆ Akenti provides data driven certificate analysis: it does no semantic analysis of the use-conditions - that is left to the resource server, or to out-of-band agreements (i.e. as to what specific terms mean and their relationships to each other).



Akenti Access Control System: Implementation



The Overall Architecture of the Authorization Certificate Approach



Akenti Access Control System

The General Security Model for Access Control

The security model is that the authorized “user community” (collection of identities that will be granted access) is defined by the intersection of a set of “use-condition” groups.

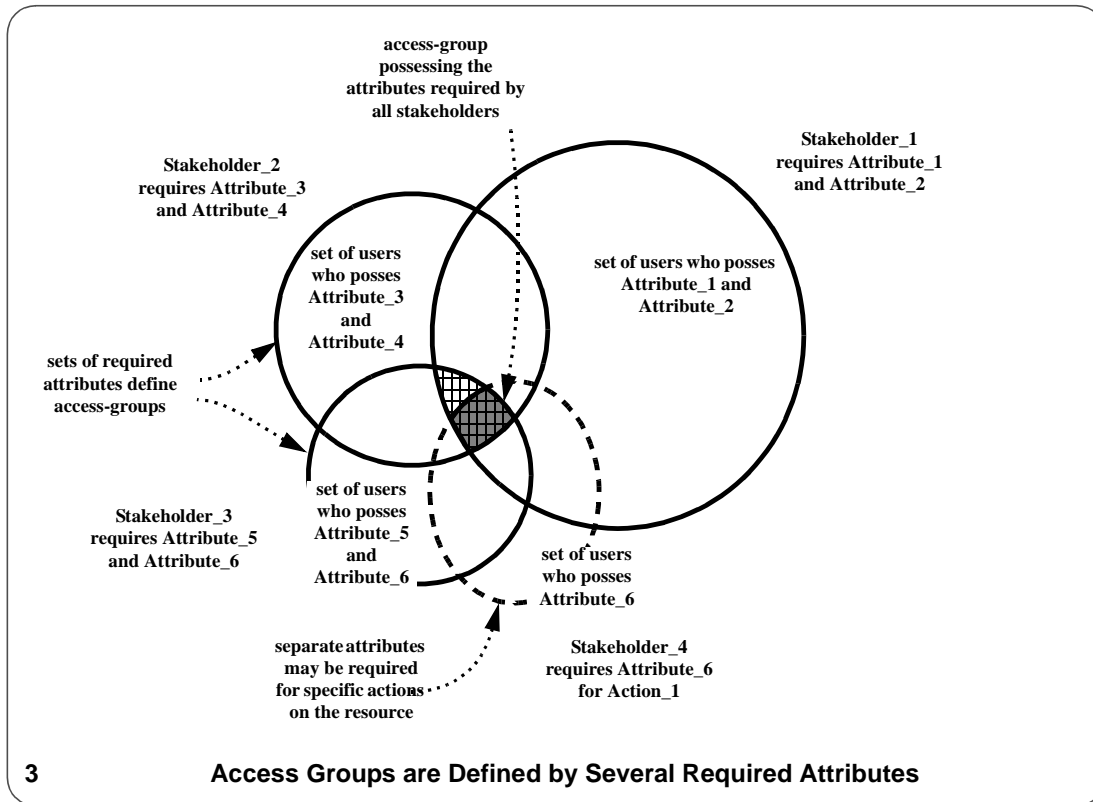
A Use-condition group is implicitly defined by a use-condition requiring an “attribute” (to be presented by a “user” in order to satisfy the use-condition).

Group are populated by designated “certifiers” who assign attributes to users.

So, the authorized community is the subset of identities that belong simultaneously to all of the use-condition groups for a resource environment.



Akenti Access Control System: Security Model



Akenti Access Control System: Security Model

This security model is intended to support a variety of policy models, including flat and hierarchical authority, and decentralized and centralized management of access conditions.

The security model provides for controlling access to resources through restrictions imposed by several types of use-conditions that are defined independently by multiple stakeholders:

- **access groups are defined implicitly by requiring a set of attributes**
- **actions on resources may be further restricted by requiring additional attributes (evaluated independently of access)**
- **operational requirements (e.g. time-of-day) are defined and satisfied by “data fields” in attribute certificates (and then acted on by the security gateway or resource server)**



Akenti Access Control System

Policy Model

A *policy model* is built on a general security model in a way that will support the access/use policies required in a particular resource domain.

The characteristics of a particular policy model - e.g. hierarchical authority with delegation - is a function of the resource / application domain.

A hierarchical policy model is implemented using the Apache Web server: the specification of resource stakeholders (i.e. who can set use-conditions) is evaluated from the point of attempted access, up to the root of the Web server directory structure. This allows for multiple, independent, hierarchically related stakeholders (who can impose use-conditions at and below the directory that they control, but not above) and it allows for delegation of authority if

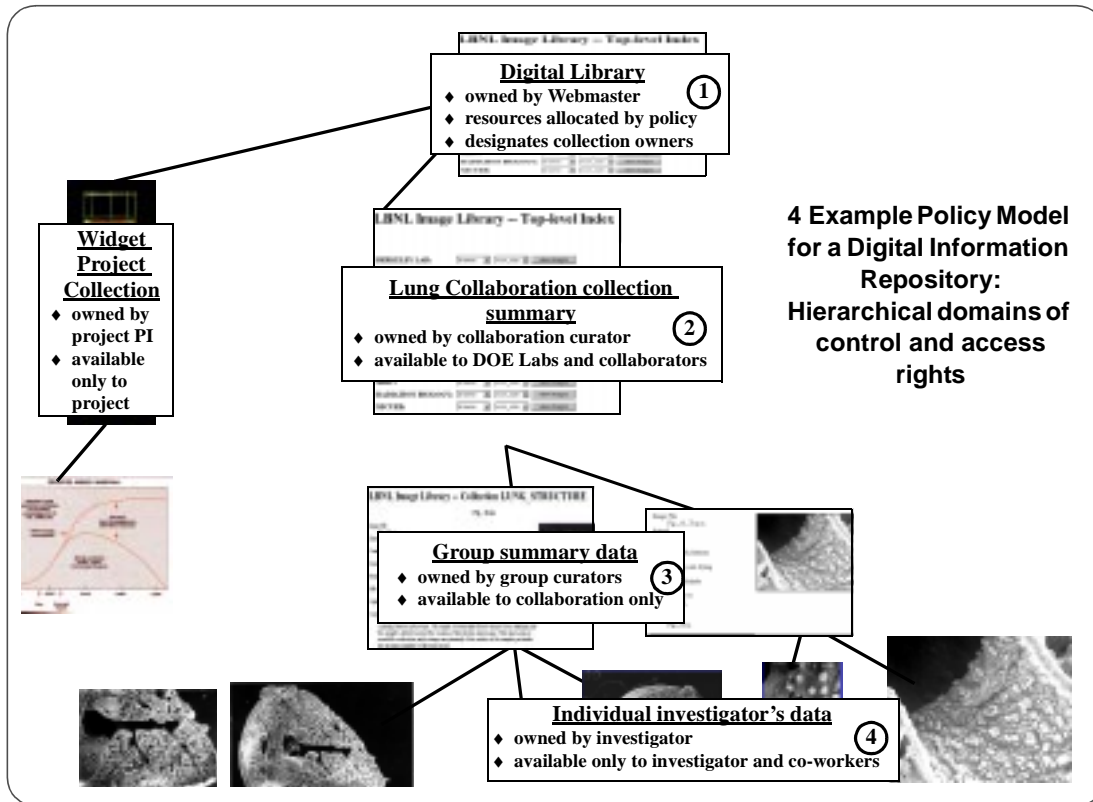


Akenti: Policy Model

the Web service (e.g. ImgLib) provides for users creating directories and specifying who can set use conditions.



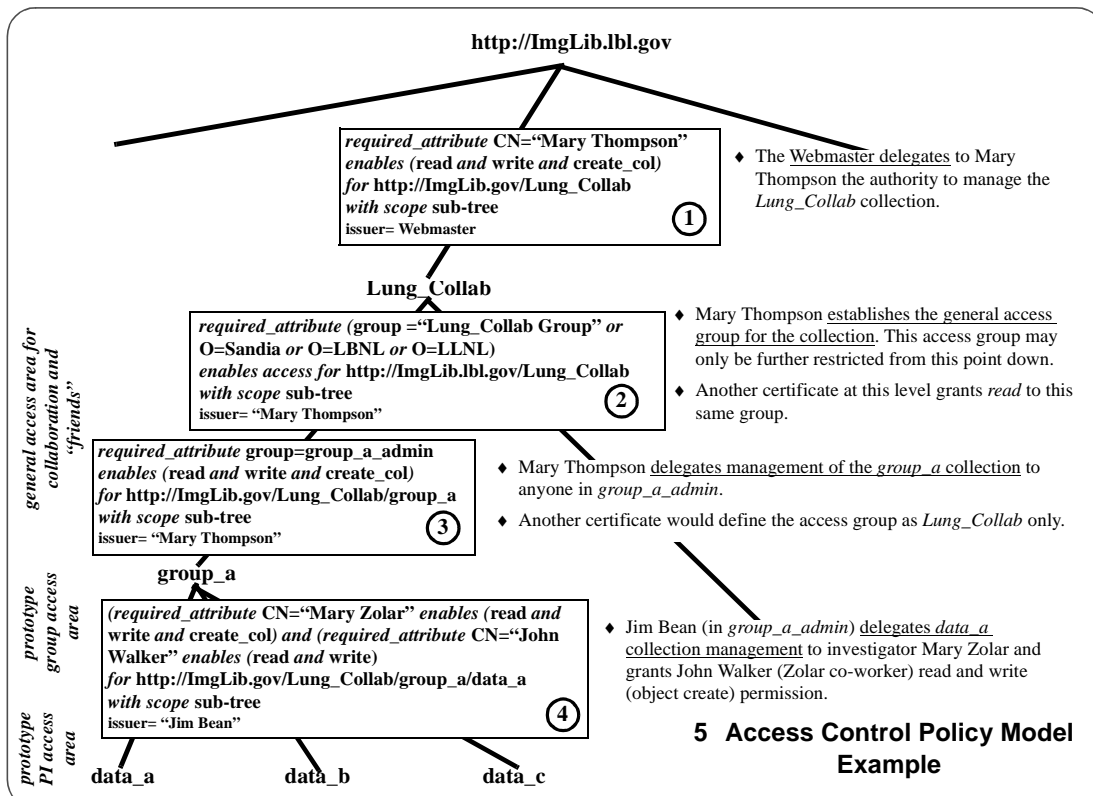
Akenti: Policy Model



4 Example Policy Model for a Digital Information Repository:
Hierarchical domains of control and access rights



Akenti: Policy Model



5 Access Control Policy Model Example



Akenti Access Control System

Operation of the Akenti Access Control System

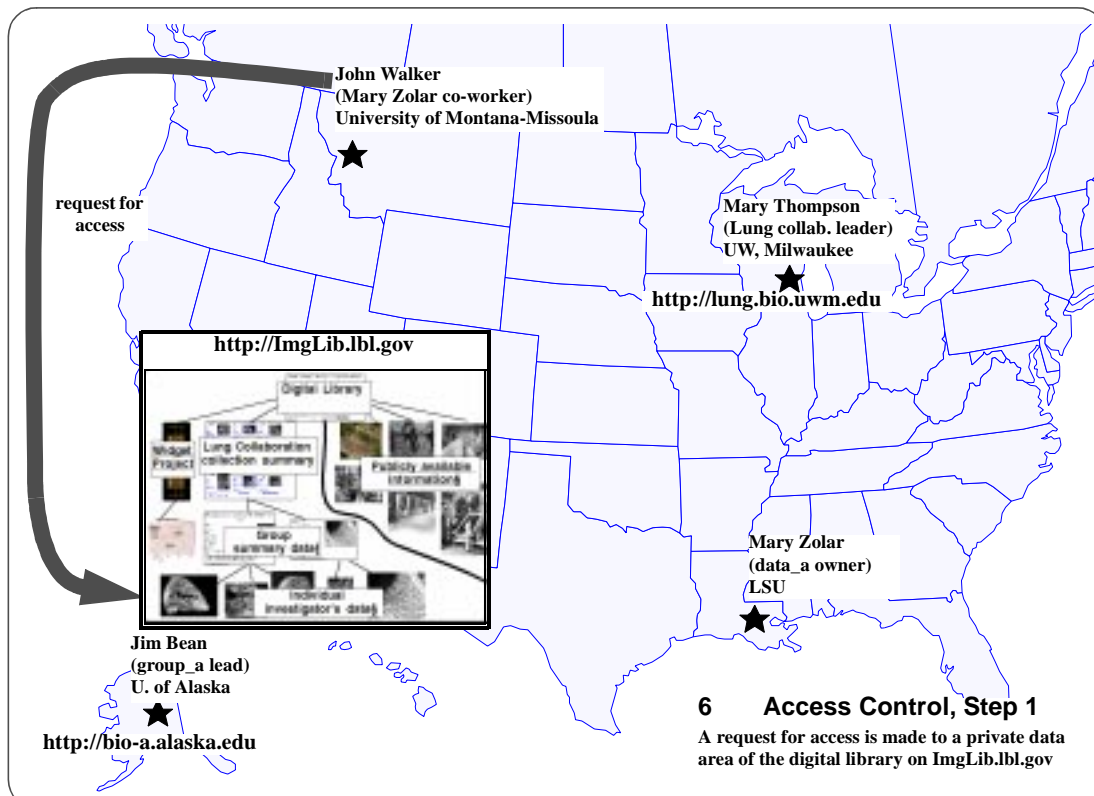
Akenti is an implementation of the “policy engine” component in the architecture illustrated in figure 2. It provides:

- an interface for acquiring a specification of the general policy items (e.g. the resource name, who are the stakeholders, which are the trusted CAs, etc.)
- acquisition and verification of all related certificates
- matching of (uninterpreted) use-conditions and attributes
- implementation of a policy model (e.g. what are the relationships among the stakeholders)
- passing the resulting “capability” to the resource controller

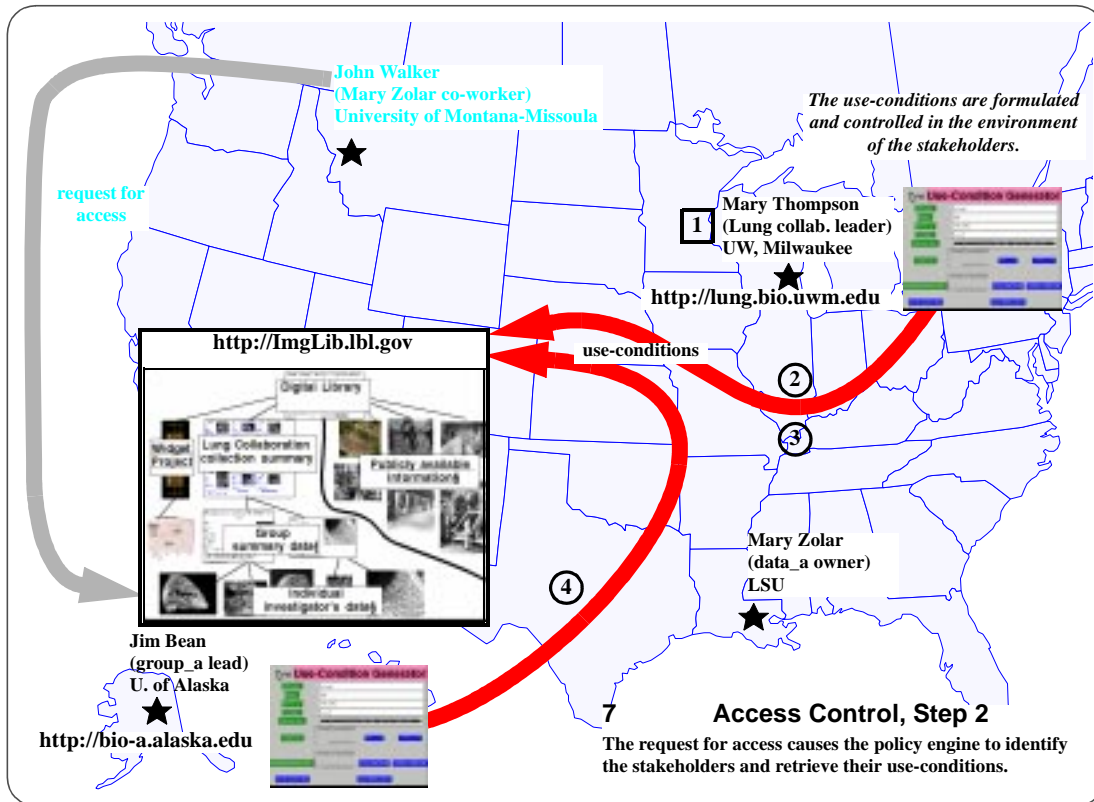
The following figures illustrate the flow of control and information in the Akenti access control system relative to the policy model illustrated in figures 4 and 5, above.



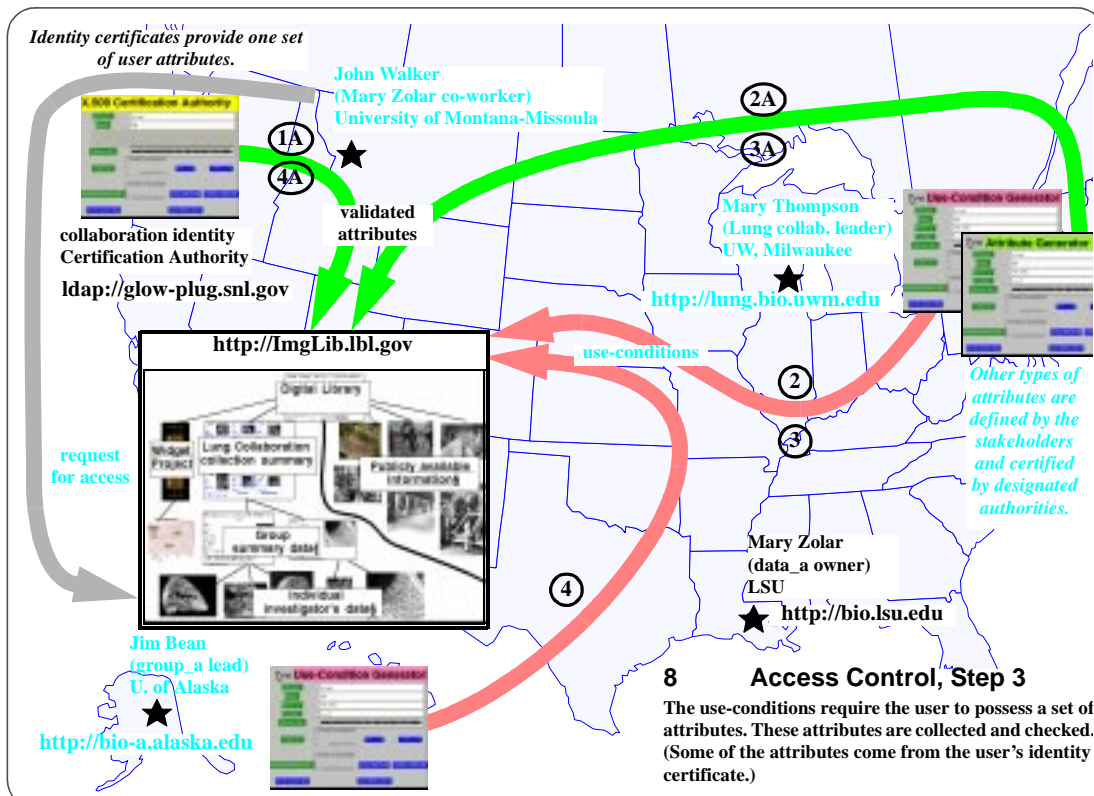
Akenti Access Control System: Operation



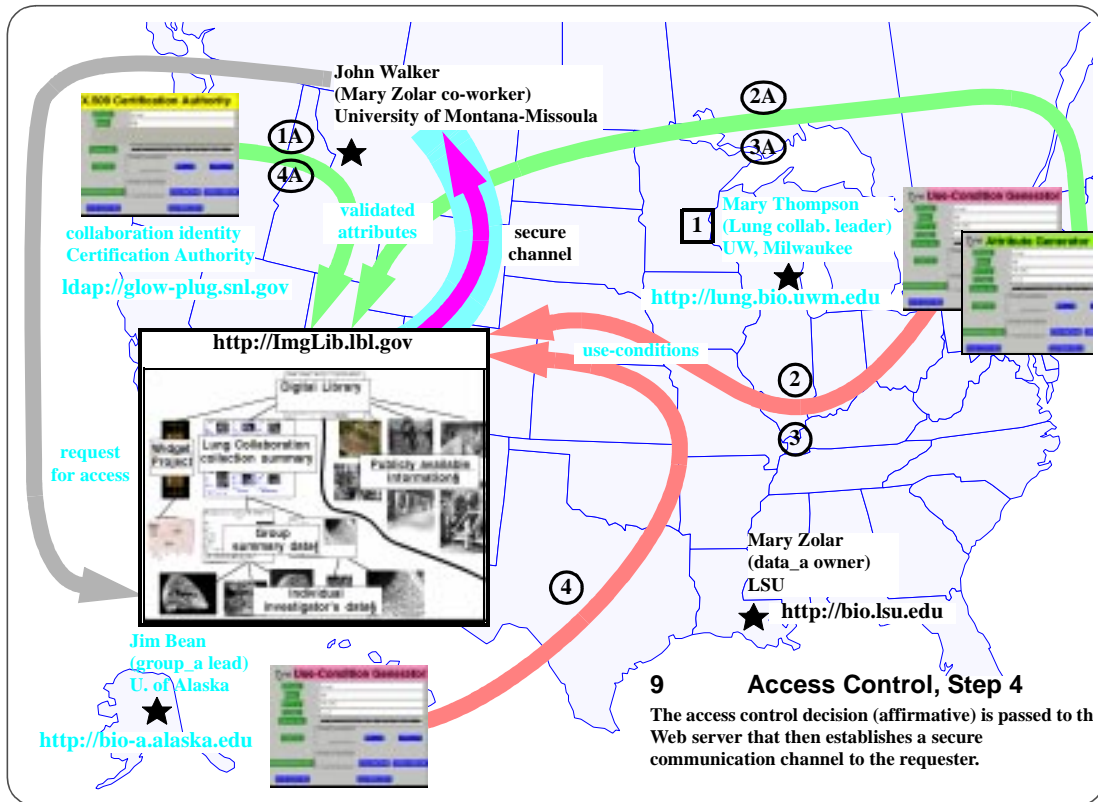
Akenti Access Control System: Operation



Akenti Access Control System: Operation



Akenti Access Control System: Operation



Akenti Access Control System

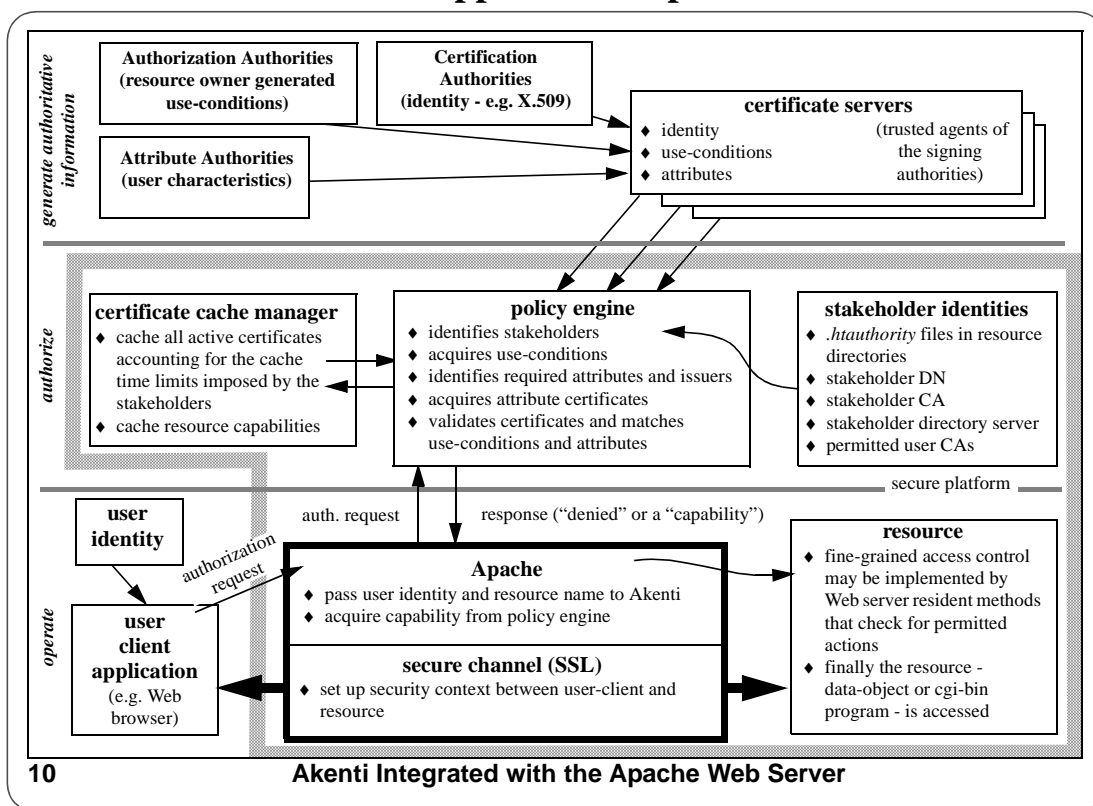
Authorization Certificates for Apache

Akenti integrates with the unmodified Apache Web server by replacing the standard access control module (“htaccess”).

Secure connection requests (https) pass the user identity certificate and the name of the requested resource to Akenti. Akenti then identifies all use-conditions, obtains the attribute certificates for the user, validates all certificates, and matches all use-conditions with attributes.



Akenti Application: Apache



Akenti Application: Apache

Identify the stakeholders (.htaauthority)

Establish explicit trust of CAs:

UserCertificateAuthority

"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"

"-----BEGIN CERTIFICATE-----\n

```
MIICdCCAd2gAwIBAgIBATANBgkqhkiG9w0BAQQFADBEMQswCQYDVQVQ
QGEwJVZuEuMCwGA1UEChMITGF3cmVuY2UgQmVya2VsZXkgTmF0aW9uYWwgTGFi
b3JhdG9yeTE
NMA\
sGA1UECxMESUNTRDEQMA4GA1UEAxMHSURDRy1DQTAeFw05NzA4MjMjMjNDJaFw05OTA4M
jMjMjNj\
MwNDJaMF4xCzAJBgNVBAYTAiVMTS4wLAYDVQQKEyVMYXZyZW5jZSBCZXJrZWxleSBOYXRpb2
5hbC\
BMYWJvcnF0b3J5MQ0wCwYDVQQLEwRJQ1NEMRAwDgYDVQQDEwJRENHUNBMIGfMA0GCS
qGSIb3DQ\
EBAQUAA4GNADCBiQKBgQDArly+tnX5eW7v4KT5CVf/IwR8rDkqniDUq34x/wqrKbM0AY+SV2hEHZ\
+MCDgSImPOXfwEplXW5IYYXqJ3+dK06et7mUodOhAB+0b6a8dVwul1+gRwEi80vft4+WvDUUHMZQ\
iq3UqFTsPN+09sW+2paqXNQZvBq2r+6/ovM4OqVwIDAQABo0IwQDADBGNVHQ4EFgQUUCQcdq1LvwV\
prM7kLIPL17fmW4PswHwYDVROjBBgwFoAUCQcdq1LvwVprM7kLIPL17fmW4PswDQYJKoZIhvcNAQ\
EEBQADgYEAtWt79TvzTI+zlKXBm8lqJPLXfsmwn0eaUGZiBkxhm5FGMU0s0sUjaAUKiC6seR9xN\
E2C6EEJ7OyZRP7agtNbbqeZBnUtCJN/iyFk9vQMMtJtTP6uBbExhUaGFuJLMhHfMG/1pfDTIHQZ\
10Q0sF1ZmLyAdhiQBxekI5c5iheP4=\n
-----ENDCERTIFICATE-----"
```

UserCertificateAuthority

"/C=US/O=Diesel Collaboratory/OU=SNL-CA/CN=glow-plug.ca.sandia.gov"

"-----BEGIN CERTIFICATE-----\n



Akenti Application: Apache

```
MIICdjCCAd+gAwIBAgIBATANBgkqhkiG9w0BAQQFADBfMQswCQYDVQ\
QGEwJVUzEdMBsGA1UEChMURGllc2VsIENvbGxhYm9yYXRvcnkxDzANBgNVBAsTBINOTC1DQTEg
MB\
4GA1UEAxMXZ2xvdy1wbHVnLmNhLnNhbmRpYS5nb3YwHhcNOTgwNDAYOTIzWhcNMDAwMz
MxMD\
AyOTIzWjBfMQswCQYDVQQGEwJVUzEdMBsGA1UEChMURGllc2VsIENvbGxhYm9yYXRvcnkxDzAN
Bg\
NVBAsTBINOTC1DQTEgMB4GA1UEAxMXZ2xvdy1wbHVnLmNhLnNhbmRpYS5nb3YwZ8wDQYJKo
ZIhV\
cNAQEBBQADgY0AMIGJAoGBAM5vxyzTTNVtEdFVS1Qnu5WXRnyxZ9RtvJQZsISRS5pG8kFi4VOYR
3\
5uOx+zjqVCaVwo+oIvKjiA2VbMe4VD5YFbxaVXmGnDDS5ct5hOh8ZSDnoOBy3dksKGkvJ8aEpOt1\
KBAPx72sWL8Jp23wCFXMCc0hFehWW2rnhkxQQ3xm7dAgMBAAAGjQjBAMB0GA1UdDgQWBBSStil15p
3\
0BaWhh17Rh4lykOgWNVjAfbgNVHSMEGDAWgBStil15p30BaWhh17Rh4lykOgWNVjANBgkqhkiG9w\
0BAQQFAAOBQAIVpDnEamYLuatyZ1xN9/q8Vf/lgoMV70Un4HYL6JvFdaDjREzzCuZLiMVUqeyN9\
oUYnAdqQ84vf4tP4mGcdq0RkG7SBaeRtMazwDfA2rLH49H+A4IVQjFjkArxg/QLa0tjVS/lkmDiV\
9A6kd+mxQb0xWohpG3QJJD7t/usI8f6g==\
-----END CERTIFICATE-----"
```

Identify directory servers for the CAs:

CertificateDirectory public ldap idcg-ds.lbl.gov

CertificateDirectory public ldap injector.ca.sandia.gov

Identify stakeholders and their certificate distribution agents:

UseConditionCAandIssuer

"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA " "/C=US/O=Lawrence
Berkeley National Laboratory/OU=ICSD/CN=Srilekha Mudumbai Authority"



Akenti Application: Apache

UseCondRequired <http://www-itg.lbl.gov/~mudumbai/Certificates>

UseConditionCAandIssuer

"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA "

"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=Mary R. Thompson-sa3"

UseCondRequired <http://www-itg.lbl.gov/~mrt/Certificates>



Akenti Application: Apache

Use-conditions:

```
<HTML>
<TITLE> Use-Condition Certificate </TITLE>
<BODY>
-----BEGIN TEXT CERTIFICATE-----
-----BEGIN TEXT-----
use-condition
issuerAndCA
"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA" "/C=US/O=Lawrence
Berkeley National Laboratory/OU=ICSD/CN=William E. Johnston sg1"
```

Identify what the use-condition is being imposed upon:

resource <http://anl-hero.es.net/bwbroker>

The policy model for this resource is hierarchical:

scope local

What is required:

attribute "(group : BWBROKER-ANL)"
enable access read,execute

Who can certify the attributes that satisfy this use-condition?

```
attributeIssuerAndCA
group "BWBROKER-ANL"
Attribute "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"
"/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=William E. Johnston sg1"
```



Akenti Application: Apache

```
subjectCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"
```

```
-----END TEXT-----
```

Assure that this certificate was issued by a legitimate stakeholder:

```
-----BEGIN SIGNATURE-----
v+TZtoZsyClhqTyYYY9/RmLHOfxY7nYewxuWJeBrT3sE/2F85jfuEHGR1/bBOz98
-----END SIGNATURE-----
-----END TEXT CERTIFICATE-----
</BODY>
</HTML>
```



Akenti Application: Apache

Attributes:

-----BEGIN TEXT ATTRIBUTE CERTIFICATE-----

attribute-certificate

What?

attribute group

value BWBROKER-ANL

When?

notValidBefore 980430233656Z

notValidAfter 980501003656Z

For whom?

subject "/C=US/O=Lawrence Berkeley National Laboratory/OU=ANL/UID=b30118/CN=Richard Carlson/Email=racarlson@anl.gov" "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=IDCG-CA"

By Whom?

issuer "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICSD/CN=William E. Johnston sg1" "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS D/CN=IDCG-CA"

Guarantee:

-----BEGIN SIGNATURE-----

dxEqG/Hsj7s1V4Gu6YTmhuReLSjPcqy3h/nDsJX9+Mr4UyOyLMHEtbbkt3uBK/yT

-----END SIGNATURE-----



Akenti Access Control System

Authorization Certificates for GSS-API

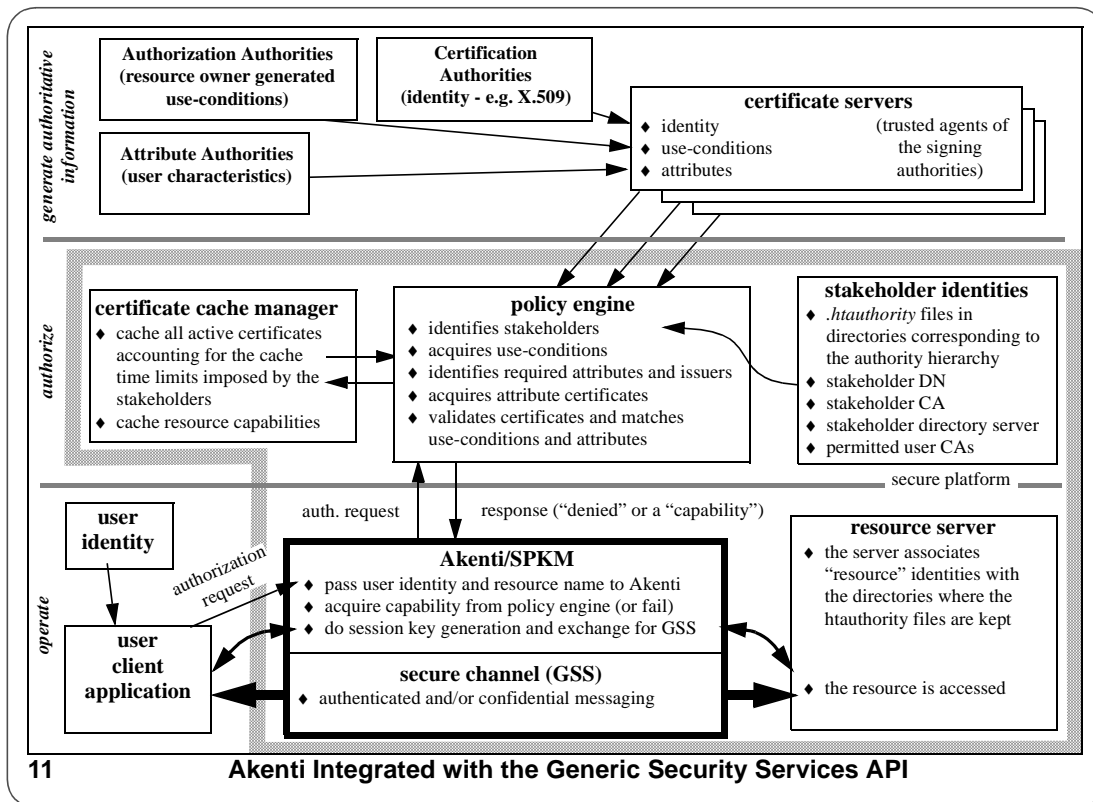
The integration of Akenti with GSS uses the Simple Public-Key Management protocol (SPKM). (SPKM is one of several standard protocols defined to do session key management for GSS.)

If the resource server has multiple functions, then these functions may be individually access controlled by imposing use-conditions on named “actions.”

If a hierarchical authority policy model is required for multiple stakeholders, then *.htaauthority* files can be placed in a directory hierarchy that is available to the resource server (actually to Akenti).



Akenti Application: GSS API



Akenti Access Control System

Authorization Certificates for CORBA

Two approaches to integration of Akenti and CORBA :

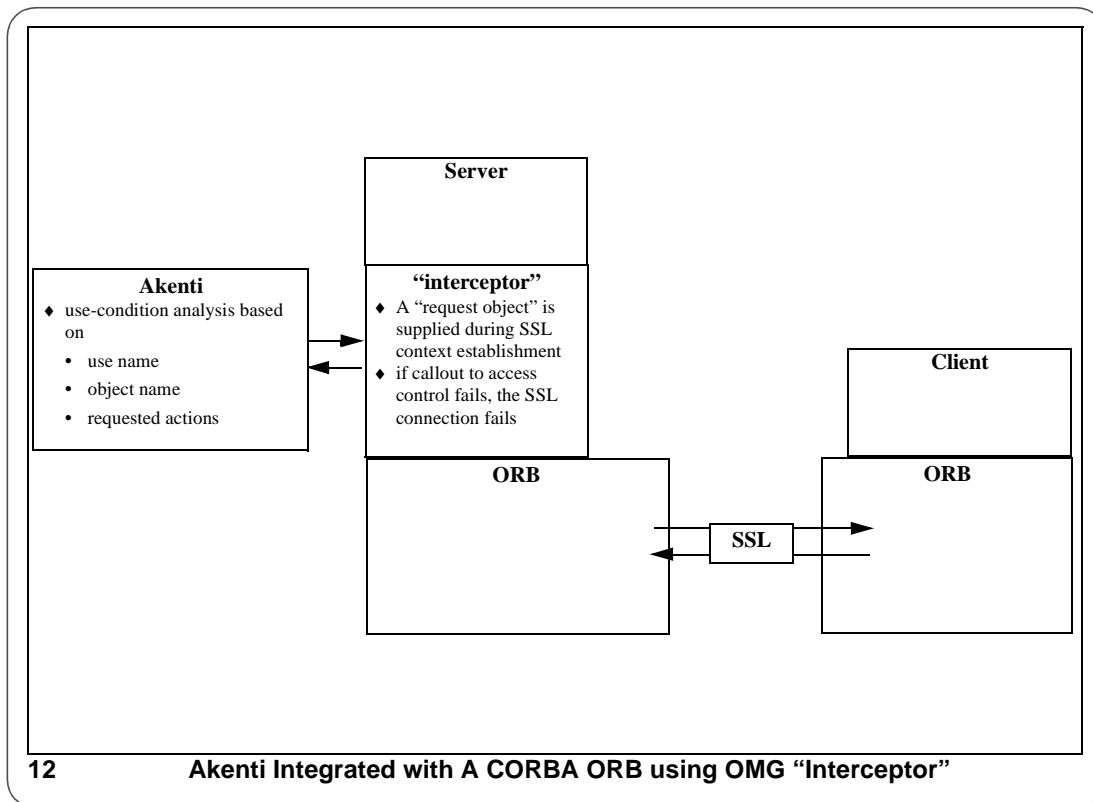
- ◆ Use Akenti+SSL
 - coarse grained — only knows server identity, not functions
- ◆ Use OMG standard “interceptor” function
 - OID
 - user/client DN

If the resource server has multiple functions, then these functions may be individually access controlled by imposing use-conditions on named “actions” that are derived from the OID.

If a hierarchical authority policy model is required for multiple stakeholders, then *.htaauthority* files can be placed in a directory hierarchy that is available to Akenti.



Akenti Application: GSS API



Akenti Access Control System

Certificate Infrastructure

How certificates are generated and managed is a key factor for the usability of the access control system:

- ♦ Must be very simple for the user
- ♦ Must be relatively simple for stakeholders
- ♦ Must not be an administrative burden

Netscape has built a useful collection of identity certificate management tools and user interfaces, and our implementation uses these facilities.

This section presents a summary of material that may be found at <http://www-itg.lbl.gov/security/Akenti>

- ♦ User Interaction
- ♦ Identity establishment
- ♦ Use-Condition generation
- ♦ Attribute Generation



Akenti: Certificate Infrastructure

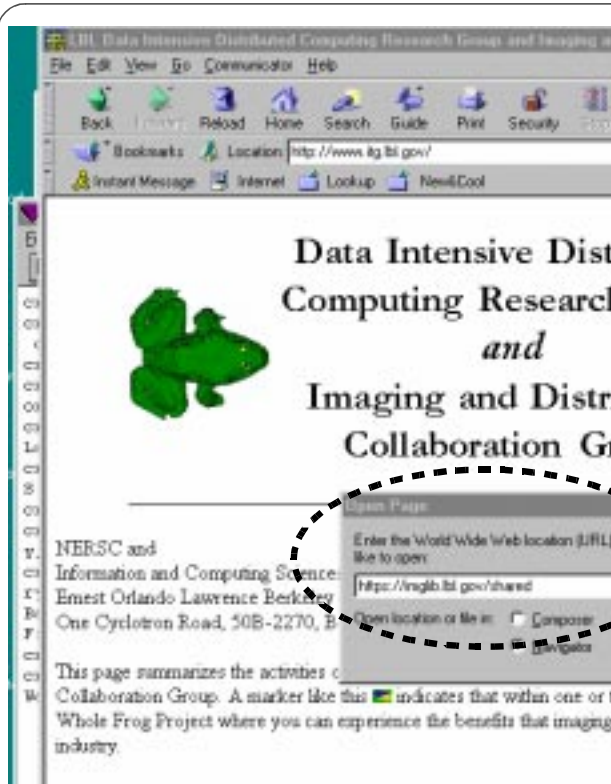
User Interaction

The normal user interaction is intended to be as transparent as possible. When attempting to access a secure resource, the user client (e.g. a Web browser) supplies the private key to authenticate the user. The access control system identifies and obtains all of the required certificates: use-conditions for the resource and the corresponding user attributes. When the use-conditions are satisfied and the user identity authenticated, access is permitted with no user action other than making the private key available.

7-UI3 8-UI4 9-UI5



Akenti: Certificate Infrastructure




Access a secure server.

Secure Web servers use the SSL (Secure Sockets Layer) protocol to authenticate the client and the server, and for setting up an encrypted communication channel. *https* refers to Web servers that use the SSL protocol. In this case, access control is provided by Akenti.



Akenti: Certificate Infrastructure



Make your identity available for authentication.

When a remote server requests your identity you must “unlock” your private key so that it may be used to authenticate your identity. (Recall that your identity is authenticated by checking that your private key and your published public key match.) Netscape allows several options for when your passphrase is requested, but at the very least it is always requested the first time that you are authenticated.


Imaging and Distributed Computing Group,
Information and Computing Sciences Division

43

[Global.Capability.Akenti.summary.VG.fm - July 22, 1998]



Akenti: Certificate Infrastructure



The user has met the use-conditions for this resource and access is allowed.

The “normal” operation of the access control system is intended to be transparent to the user, and specific use-conditions are not normally visible to the user. The use-conditions, and the user attributes needed to satisfy them, are established elsewhere. (However if “real” credentials beyond identity are required for a particular resource, then the user will have to provide those to the party who is certifying that user attribute.)

Imaging and Distributed Computing Group,
Information and Computing Sciences Division

44

[Global.Capability.Akenti.summary.VG.fm - July 22, 1998]



Akenti: Certificate Infrastructure


Identity Establishment

An identity certificate binds a user name to a public key in a document issued by a trusted third-party (the Certification Authority.) The private key and the public key are cryptographically bound - what one encrypts only the other can decrypt. It is this binding that allows the private key - if it has been held in confidence by its owner - to strongly authenticate the owner to anyone who obtains the owner's public key from the CA.

4 5



Akenti: Certificate Infrastructure



The Certification Authority issues identity certificates to users.

The CA will have a published policy on what is required of the user in order to receive a certificate. The request is received by the CA administrator and held until the identity verification process has been completed.



Akenti: Certificate Infrastructure

The user supplies the basic information for a certificate

“Your Full Name” becomes your “Common Name” in the X.509 certificate. If the same CA issues you multiple certificates, then the names must be unique.

The exact form of “Org. Unit”, “Org.”, and “Country” must be obtained from the CA administrator.



Akenti: Certificate Infrastructure

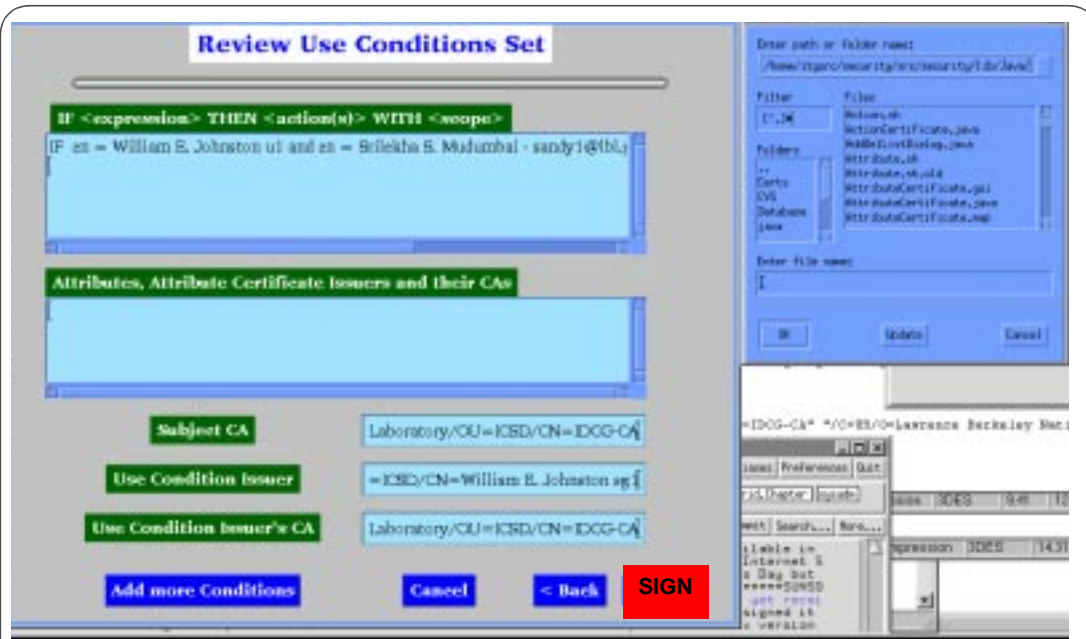
Use-conditions

A resource stakeholder (e.g. data “owner”) will impose use-conditions that must be met before access is allowed. Akenti provides several forms of use-conditions. Example use-conditions:

- ◆ Some component of an X.509 certificate (e.g. “organization” - fairly general or “common name” - very specific)
(in this case the X.509 certificate supplies all of the required attributes)
- ◆ Group membership
(stakeholders can establish their own groups, and attribute certificates issued by parties named by the stakeholder will place a user into the group - i.e., an attribute certificate issued to a user that attests to membership in the group)



Akenti: Certificate Infrastructure



The completed use-condition certificate (requiring an X.509 component in this case) is signed by the stakeholder and made available by a trusted server.



Akenti: Certificate Infrastructure

Attributes

Attributes are provided by certifiers trusted by the use-condition issuer. Formally, attributes are associated with users, not with resources. (Though specific groups may be associated with specific resources.)



Akenti: Certificate Infrastructure

Preview and Generate Attribute Certificate

Preview the requirements for generating an attribute certificate and if satisfied, sign it.

Attribute group

Value HPSS

SubjectAndCA Mary R. Thompson, IDOG-CA

AttributeIssuerAndCA William E. Johnston sgl, IDOG-CA

Cancel < Back Sign Certificate

The attribute certificate is constructed and signed.



Akenti: Certificate Infrastructure

Resource

Enter path or folder name: /home/2/users/johnston/public_html/Certificates

Filter: [*.*]

Files: R.S. Building.gif, R.S. Tech.gif, R.S. Tech.ps, RP11.1.0-04.fw.ps, RP11.1.0-04.fw.pdf, RP11.1.3-04.fw.ps, RP11.1.3-04.fw.pdf, RP11.1.3.fw.pdf

Folders: CERNSchool, Certificates, Exp.Grid, Dnsel

Enter file name: thompson-ingsib.shared.w

OK Update Cancel

The certificate is “published”.

The location of attribute certificates is an important part of the assurance process. The signing authority must designate one or more trusted servers for publishing attribute certificates. These servers are “trusted” not because a certificate can be counterfeited (extremely difficult - impossible with ordinary resources - because of the cryptographic strength of public-key cryptography) but because the absence of a certificate from the designated server (usually the certifier’s Web server) denies access to a user.



CDS: A Simple Akenti Application

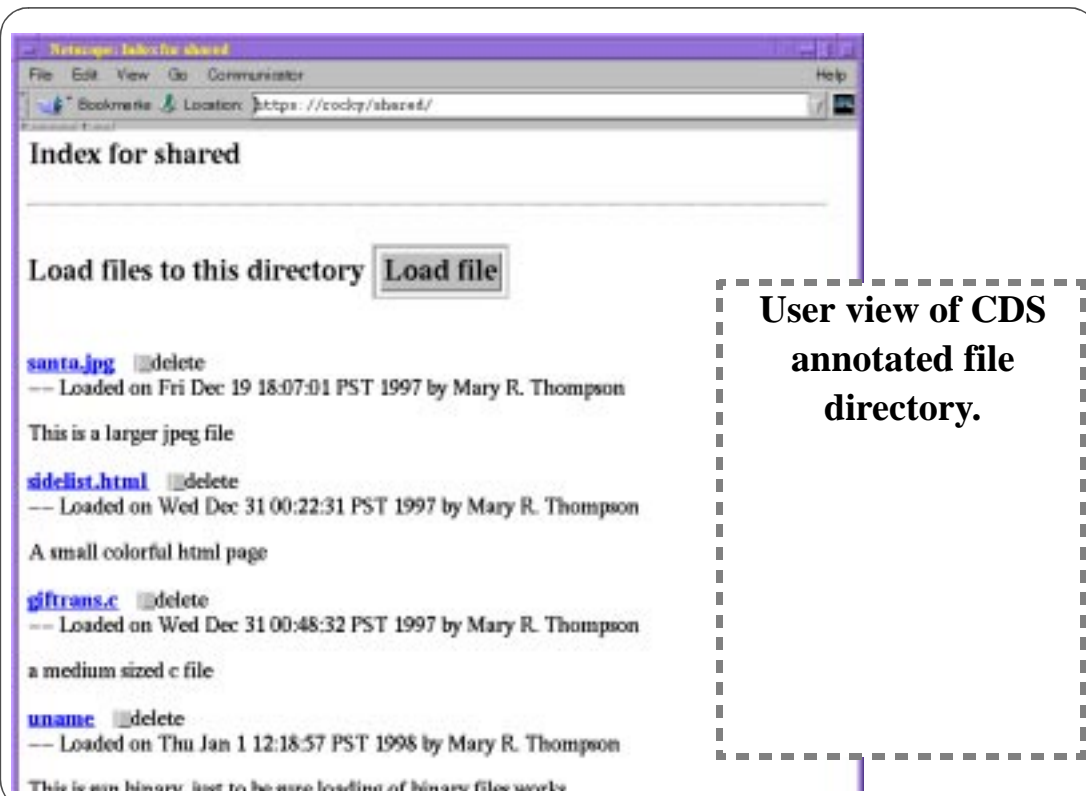
CDS (access *Controlled Data Sharing*) provides a simple interface for uploading and downloading files to and from an area of a server that is access controlled by use-condition certificates.

The file appears on a Web page, and may be described by a simple annotation.

The goal is a secure and easily used, group-oriented, data sharing facility.



Akenti: Application



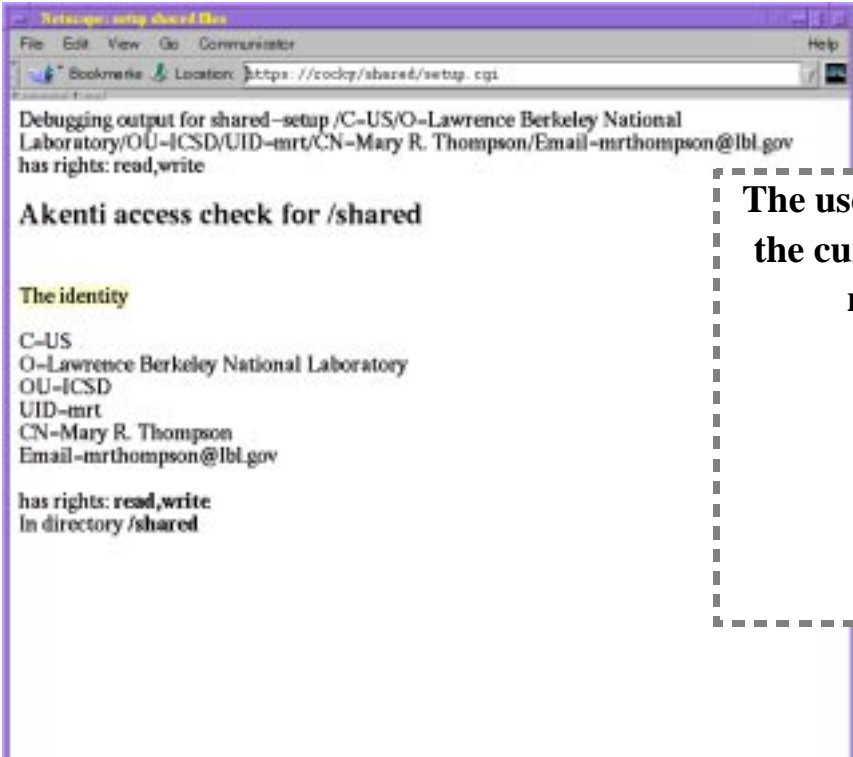
The screenshot shows a Netscape browser window with the address bar set to <https://cocky/shared/>. The page title is "Index for shared". Below the title, there is a section "Load files to this directory" with a "Load file" button. The main content area lists four files, each with a "delete" button and a description:

- [santa.jpg](#) delete
--- Loaded on Fri Dec 19 18:07:01 PST 1997 by Mary R. Thompson
This is a larger jpeg file
- [sidelist.html](#) delete
--- Loaded on Wed Dec 31 00:22:31 PST 1997 by Mary R. Thompson
A small colorful html page
- [giftrans.c](#) delete
--- Loaded on Wed Dec 31 00:48:32 PST 1997 by Mary R. Thompson
a medium sized c file
- [uname](#) delete
--- Loaded on Thu Jan 1 12:18:57 PST 1998 by Mary R. Thompson
This is an binary list to be used loading of binary files

A dashed box on the right side of the screenshot contains the text: "User view of CDS annotated file directory."



Akenti: Application



Debugging output for shared-setup /C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/UID=mrt/CN=Mary R. Thompson/Email=mrthompson@lbl.gov
has rights: read,write

Akenti access check for /shared

The identity

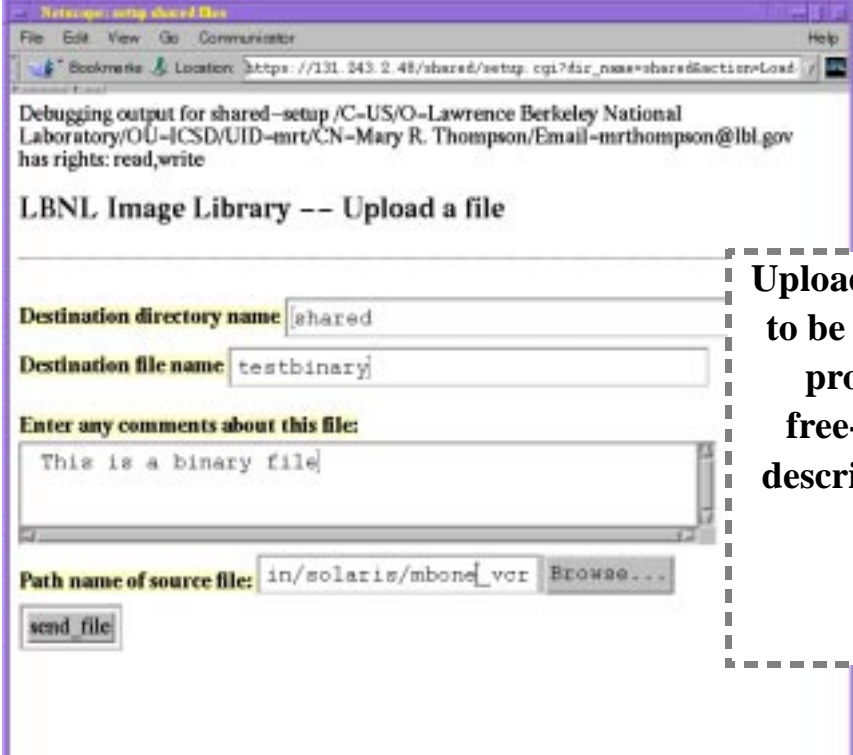
C=US
O=Lawrence Berkeley National Laboratory
OU=ICS
UID=mrt
CN=Mary R. Thompson
Email=mrthompson@lbl.gov

has rights: read,write
in directory /shared

The user can query the current access rights.



Akenti: Application



Debugging output for shared-setup /C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/UID=mrt/CN=Mary R. Thompson/Email=mrthompson@lbl.gov
has rights: read,write

LBNL Image Library -- Upload a file

Destination directory name:

Destination file name:

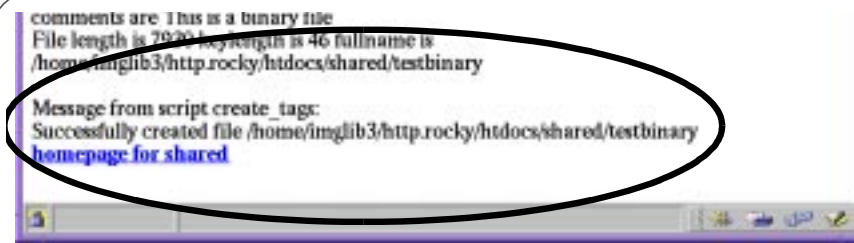
Enter any comments about this file:

Path name of source file:

Upload is intended to be simple, and provides for free-form user description of the file.



Akenti: Application



**Filtering the audit
log will provide user
feedback.**




Akenti: Application



**A new shared file has
been created.**



Akenti: Application

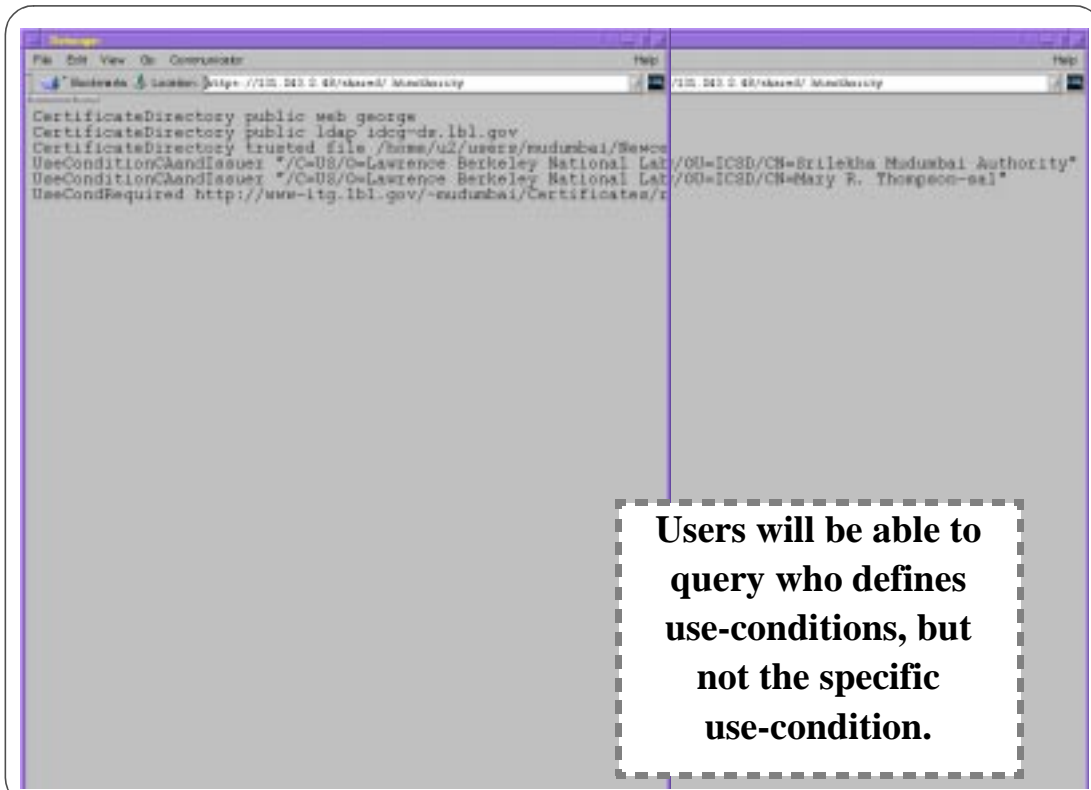


The screenshot shows a web browser window with the URL `https://today/shared/setup.cgi?dir_name=shared&delete_file=xxxxxx`. The page content includes a debugging output for a shared setup, a title "LBNL Image Library -- Delete a file", and a confirmation message: "Do you really want to delete the following file(s) from shared". Below this, there are input fields for "uname" and "anewfile", a "DELETE" button, and a "Go Back" link.

Delete capability is granted separately from access.



Akenti: Application



The screenshot shows a web browser window with the URL `https://133.243.5.48/shared/MenuLibrary`. The page content displays a list of use conditions, including "CertificateDirectory public web george", "CertificateDirectory public ldap idcg-ds.lbl.gov", "CertificateDirectory trusted file /home/u2/users/madumbai/Bewce", "UseConditionCaandIssuer */C=US/O=Lawrence Berkeley National Lab/OU=ICSD/CN=Brillatha Madumbai Authority", "UseConditionCaandIssuer */C=US/O=Lawrence Berkeley National Lab/OU=ICSD/CN=Mary R. Thompson-sal", and "UseCondRequired http://www-itg.lbl.gov/~madumbai/Certificates/r".

Users will be able to query who defines use-conditions, but not the specific use-condition.



Bandwidth Reservation

We propose a model for bandwidth reservation that can be used in the context of a general resource reservation scheme, but at the same time stay within the scalable model of the differentiated classes of service as described in the IETF diffserv Working Group documents ([5]).

The basic idea is to have bilateral end node agreements that “reserve” bandwidth in the sense that a site actively manages allocation against one or more classes of service. The overall limits on a class of service are established in the corresponding service-level agreement between the institution of the end nodes and the ISP, but the allocation of flows to this class is closely managed by the end node institutions at the site egress.

Further, the resource allocation should be policy based in a way that allows automated reservation, and it should also be possible to proxy one’s policy based authority to another site so that the bilateral agreements necessary for inter-site application operation happen automatically. (See, e.g., [2].)

The network level technology to accomplish this is provided by the classifier/shaper/policer functions of the diffserv “traffic conditioner” (TC) element. Layered on top of the TC is a “slot” allocation mechanism (“bandwidth manager”) that manages the use of a service class. When instantiated, this slot is a “micro flow” in the diffserv terminology.

Reservation requests are made to the bandwidth manager. The identity of the requestor (user_A), together with the requested resource (time slot, source id, bandwidth) are compared with policy. If the requestor and resource meet the policy, a reservation is made (the slot is allocated and the available bandwidth in the SLA is decremented) and a certificate (a digitally signed document) is issued by the bandwidth manager to represent the reservation.

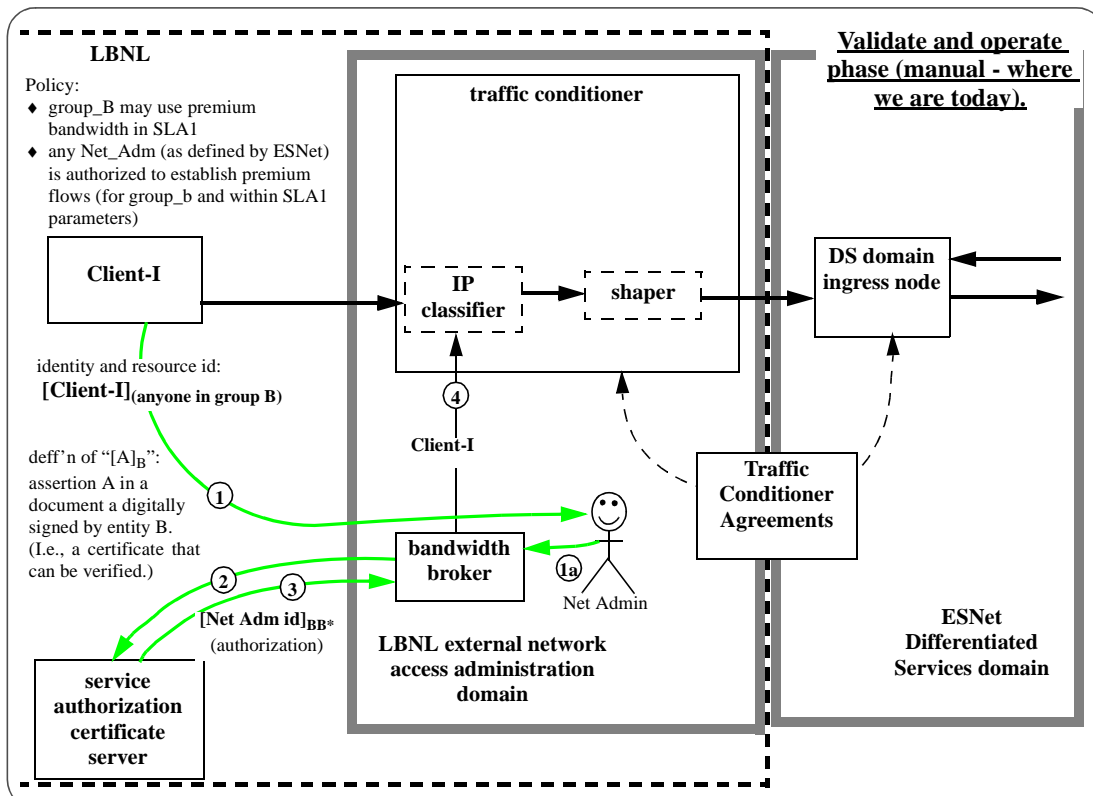
When, at some point in the future, a request is made to instantiate the flow (i.e. start the instrument or application) the bandwidth manager retrieves the certificate (based on the requestor id and flow characteristics), validates the user and certificate, and instantiates the flow.

The flow characteristics are passed to the TC for classification and enforcement. From the point of view of the ingress router of the ISP, the SLA is never violated because the site bandwidth manager does not over allocate and the TC enforces flow characteristics as reserved.

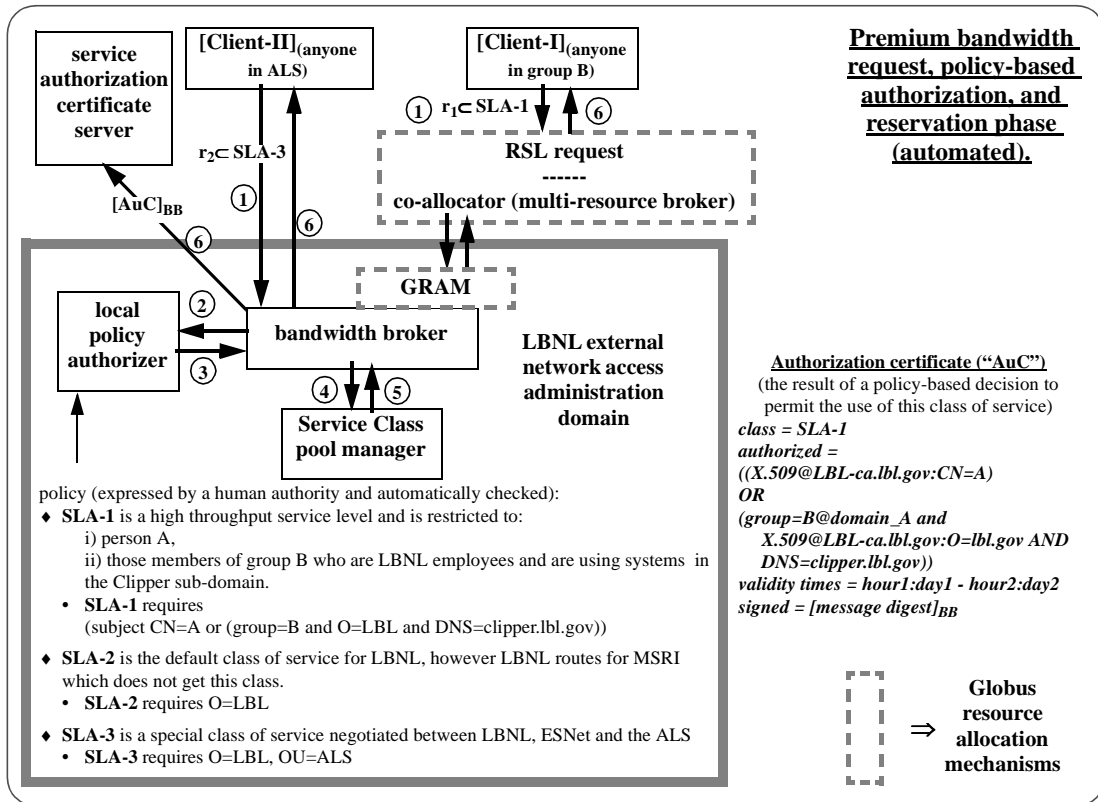
Another important component in this architecture is a bandwidth broker. This service interacts with the bandwidth manager at the target site in order to accomplish the bilateral reservation. The model here is that some entity (“user_B”) at the target site (“site_B”) is the (willing) receiver of the flow. The site_B entity must have the right (i.e., be within the policy of site_B) to utilize this flow. User_B conveys (a priori) its authority (in the form of a proxy certificate) to user_A, and the site_A bandwidth broker presents this proxy to the site_B bandwidth manager in order to accomplish the reservation. The site_B incoming flow could probably just be authenticated based on the flow spec matching the reservation (i.e., site_B trusts site_A to authenticate the flow when it is instantiated), although more elaborate authentication is possible.



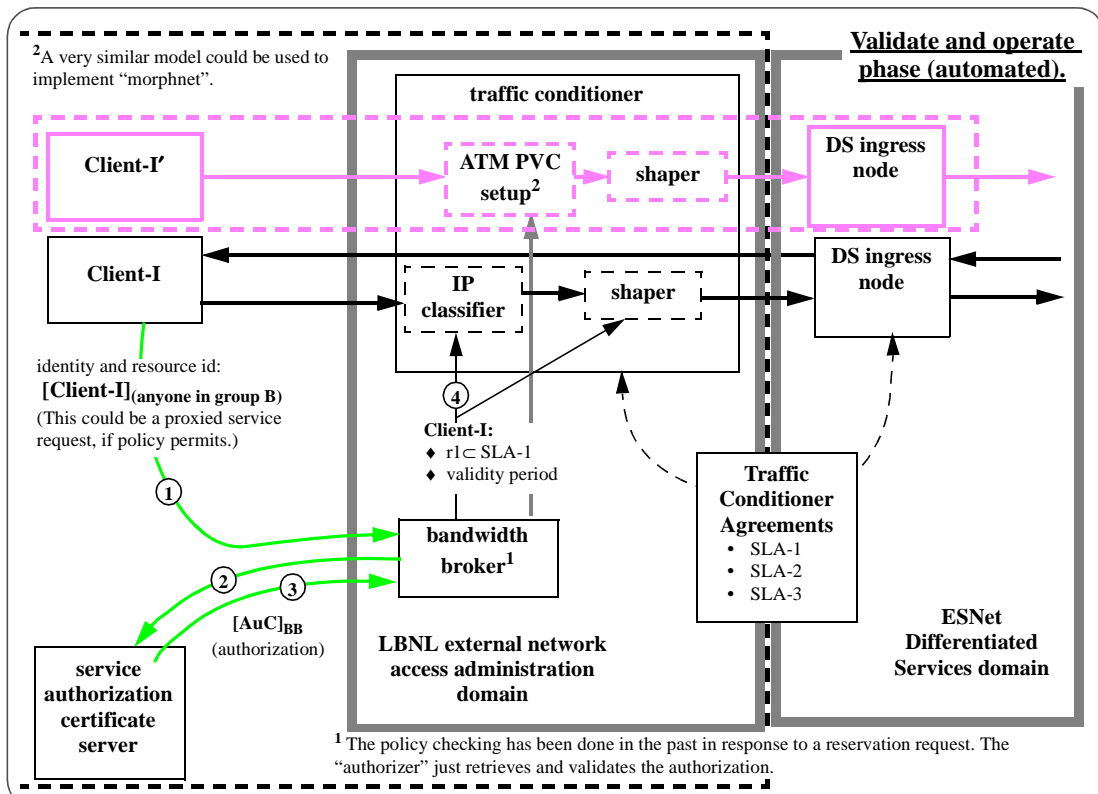
Akenti Application: Bandwidth Reservation



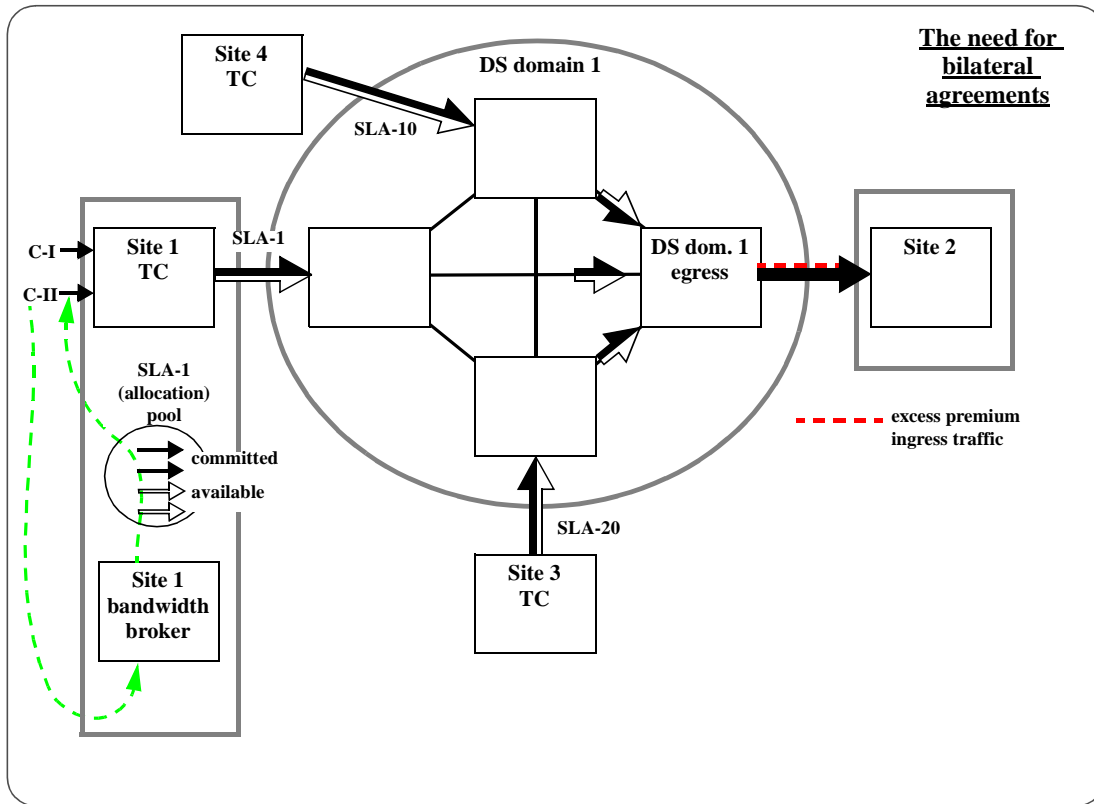
Akenti Application: Bandwidth Reservation



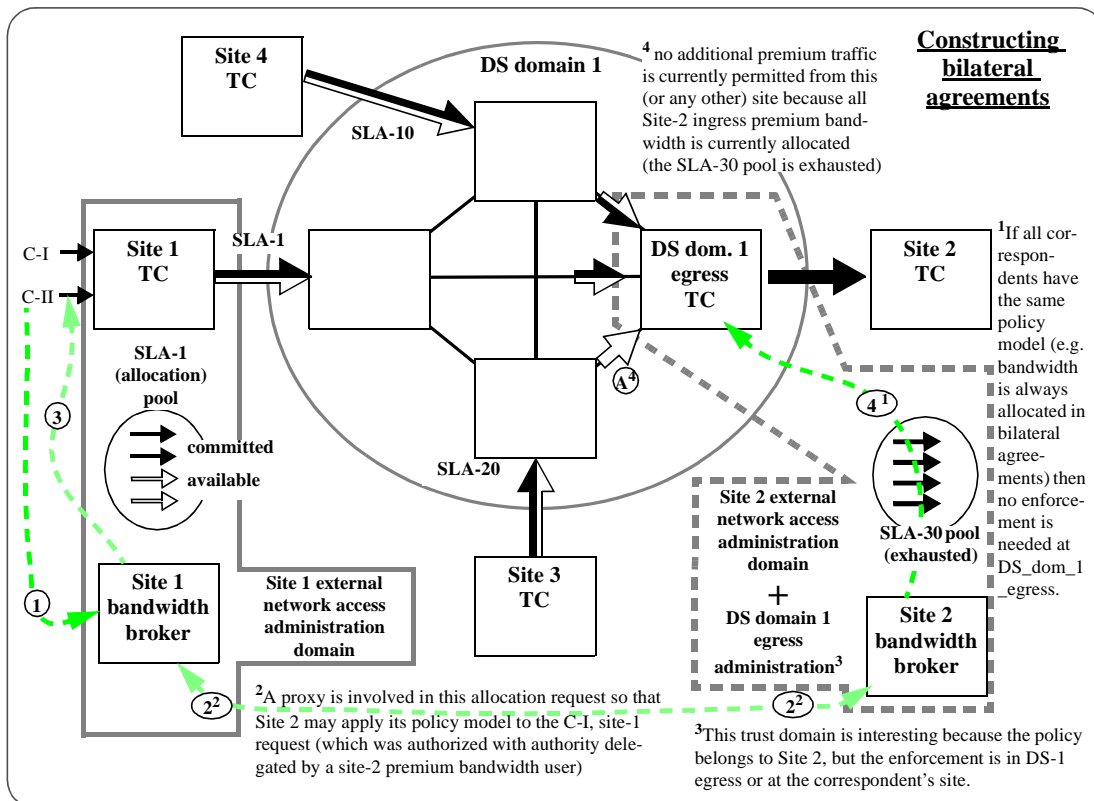
Akenti Application: Bandwidth Reservation



Akenti Application: Bandwidth Reservation



Akenti Application: Bandwidth Reservation



Monitoring

The NetLogger [1] event monitoring system is being used to track and record all “events” — acquisition of policy “elements,” and their corresponding certificates.



Akenti Application: Monitoring

Akenti access check for <http://imglib.ill.gov/shared/web/>

The identity
/CN=US/CN=Lawrence Berkeley National Laboratory/CN=O=JED=us/CN=William E. Johnston/CN=mail@imglib.ill.gov

has rights: none

[Log In](#)

STATUS PANELS

Collecting policy elements ...

Validating site conditions ...

Satisfying access use conditions ...

DIRECTORY SERVICES

Resource=/home/imglib3/http/imglib3/htdocs/shared/web/
CertificateDirectory: public idag idagm3.ill.gov
CertificateDirectory: trusted file /home/a2/users/johnston/public_html/

Resource=/home/imglib3/http/imglib3/htdocs/shared/
CertificateDirectory: public idag idagm3.ill.gov
CertificateDirectory: trusted file /home/a2/users/madsamba/keys/certs
CertificateDirectory: trusted file /home/a2/users/ent/public_html/WWW/

Resource=/home/imglib3/http/imglib3/htdocs/
CertificateDirectory: public idag idagm3.ill.gov

User-level Access Checking.
(An Applet invoked from an access controlled Web server.
Even to get this, the user must have an identity certificate
from a trusted CA.
Each colored box results from analyzing a policy element.
The corresponding certificates are displayed on the right.
Clicking on the box will show the policy element.)



Akenti Application: Monitoring

```
Akenti policy files for http://imglib.lbl.gov/shared/wej

The identity
/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/UID=wej/CN=William E. Johnston/Email=wej@lbl.gov

has the rights: none

The policy file for shared/wej is:

CertificateDirectory public ldap idag-ds.lbl.gov
CertificateDirectory trusted file /home/u2/users/johnston/public_html/Certificates
UseConditionAndIssuer "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA"
UseCondRequired http://www-itg.lbl.gov/~johnston/Certificates/

Pulling UseConditionCertificate http://www-itg.lbl.gov/~johnston/Certificates/
reqstr is: GET /~johnston/Certificates/ HTTP/1.0
Pulling UseConditionCertificate http://www-itg.lbl.gov/~johnston/Certificates/40256262.0
reqstr is: GET /~johnston/Certificates/40256262.0 HTTP/1.0

Use Condition Certificate is:

-----BEGIN TEXT CERTIFICATE-----
-----BEGIN TEXT-----
use-condition
issuerAndCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA"
attribute "group : HPSS"
resource http://imglib.lbl.gov/shared/wej
scope sub-tree
enable access read,write,modify,chmod
subjectCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA"
attribute issuerAndCA group Attribute "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA"
-----END TEXT-----
-----BEGIN SIGNATURE-----
(MIsQ3064CPX)/d48wQx6MvntZReedG WswsEzP2PpH7gsYXeyf05E
-----END SIGNATURE-----
-----END TEXT CERTIFICATE-----
```

Administrator-level Policy Checking.

(Essentially a real-time display of the Akenti log.)



Akenti Application: Monitoring

```
The policy file for shared is:

#CertificateDirectory public web george
CertificateDirectory public ldap idag-ds.lbl.gov
CertificateDirectory trusted file /home/u2/users/mudumbai/Newerts
CertificateDirectory trusted file /home/u3/users/mrt/public_html/Attributes
UseConditionAndIssuer "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA"
UseCondRequired http://www-itg.lbl.gov/~mrt/Certificates/

Pulling UseConditionCertificate http://www-itg.lbl.gov/~mrt/Certificates/
reqstr is: GET /~mrt/Certificates/ HTTP/1.0
Pulling UseConditionCertificate http://www-itg.lbl.gov/~mrt/Certificates/5862edd0.0
reqstr is: GET /~mrt/Certificates/5862edd0.0 HTTP/1.0

Use Condition Certificate is:

-----BEGIN TEXT CERTIFICATE-----
-----BEGIN TEXT-----
use-condition
UID "mrt@lbl.gov#5862edd0#Wed Jun 10 14:16:35 PDT 1998"
issuerAndCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA"
resource http://imglib.lbl.gov/shared
scope sub-tree
attribute "group : IDOG"
enable read,write,modify,chmod
attribute issuerAndCA group "IDOG" Attribute "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA" "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA"
subjectCA "/C=US/O=Lawrence Berkeley National Laboratory/OU=ICS/CN=IDOG-CA"
subjectCA "/C=US/O=Diesel Combustion CoLaboratory/OU=SNL/CN=DieselCert.ca.sandia.gov"
-----END TEXT-----
-----BEGIN SIGNATURE-----
TYLPPGKqpeAbelcFXLa4NpqpDQZmJp=ZOGI2A2A,jafuL,Mgnyf=0VLXJdLrptJRYFDCKHUQ6h
6477kErmBjpsHMadSL6jgrPv483uJ/vcNY5U2BdHWSq81tylthd0dms+cmqrgJBrmhk5HW/
uwqR8Qhg8LW6AHgD=
-----END SIGNATURE-----
-----END TEXT CERTIFICATE-----
```



Akenti Application: Monitoring

The rest policy is in:

[illegible]

Akenti Application: Monitoring

Use Condition Certificate in

```
-----BEGIN TEXT CERTIFICATE-----
-----BEGIN TEXT-----
use-condition
UID "ydcy:lbl.gov#0ba59106#Wed Jun 10 14:00:13 PDT 1998"
issuerAndCA "/C=US/O=Lawrence Berkeley National Laboratory/CN=4CSD/CN=4DCG-CA" /C=US/O=Lawrence Berkeley National Laboratory/CN=4CSD/CN=4DCG-CA
resource http://imglib.lbl.gov
scope sub-tree
attribute "[] o : Lawrence Berkeley National Laboratory or o : Diesel Combustion Collaboratory]"
enable access read execute
attribute issuerAndCA "Lawrence Berkeley National Laboratory" X509 "/C=US/O=Lawrence Berkeley National Laboratory/CN=4CSD/CN=4DCG-CA"
attribute issuerAndCA "Lawrence Berkeley National Laboratory" X509 "/C=US/O=Lawrence Berkeley National Laboratory/CN=4CSD/CN=4DCG-CA"
attribute issuerAndCA "Diesel Combustion Collaboratory" X509 "/C=US/O=Diesel Combustion Collaboratory/CN=5NL/CN=DieselCert.ca.sandia.gov"
attribute issuerAndCA "Diesel Combustion Collaboratory" X509 "/C=US/O=DieselCert.ca.sandia.gov"
subject CA "/C=US/O=Lawrence Berkeley National Laboratory/CN=4CSD/CN=4DCG-CA"
subject CA "/C=US/O=Diesel Combustion Collaboratory/CN=5NL/CN=DieselCert.ca.sandia.gov"
-----END TEXT-----
-----BEGIN SIGNATURE-----
ESW=dK1aML6Q7eP9pLRSQ$99mK17Kd/aGdL-180/LP7WELx0C6-8W8pb0756dnY2BkLhwmc
GEVcG/GBMBoXVdL+GbnHmHAcnDgtKWU3LsWpzm/m7C04C2HcK5gN8egp8srkUfz2P8-S1YE2ek
#D8bGtGdLn7brie=
-----END SIGNATURE-----
-----END TEXT CERTIFICATE-----
```



Akenti Application: Monitoring

Notes

Unless otherwise noted, these paper are on the Web, and pointers may be found at <http://www-itg.lbl.gov/~johnston/papers> .

- [1] **"The NetLogger Methodology for High Performance Distributed Systems Performance Analysis,"**
Brian Tierney, W. Johnston, J. Lee, G. Hoo, C. Brooks, D. Gunter. 7th IEEE Symposium on High Performance Distributed Computing, Chicago, Ill. July 29-31, 1998.
- [2] **"Authorization and Attribute Certificates for Widely Distributed Access Control,"**
William Johnston, S. Mudumbai, and M. Thompson. IEEE 7th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises - WETICE'98, Stanford, CA. June, 1998.
- [3] **"Real-Time Generation and Cataloguing of Large Data-Objects in Widely Distributed Environments,"**
W. Johnston, Jin G., C. Larsen, J. Lee, G. Hoo, M. Thompson, and B. Tierney (LBNL) and J. Terdiman (Kaiser Permanente Division of Research). Invited paper, International Journal of Digital Libraries - Special Issue on "Digital Libraries in Medicine". May, 1998.
- [4] **Akenti**
PKI, Attribute, and Use-Condition certificate based access control with distributed management of multi-party policy.
See <http://www-itg.lbl.gov/security/Akenti>
- [5] **diffserv**
"There is a clear need for relatively simple and coarse methods of providing differentiated classes of service for Internet traffic, to support various types of applications, and specific business requirements. The differentiated services approach to providing quality of service in networks employs a small, well- defined set of building blocks from which a variety of services may be built."
<http://www.ietf.org/html.charters/diffserv-charter.html>
- [6] **WALDO**
"The Wide Area Large Data Object Architecture: We are exploring the use of highly distributed computing and storage architectures to provide all aspects of collecting, storing, analyzing, and accessing large data-objects. These data-objects can be anywhere from tens of MBytes to tens of GBytes in size. They are typically the result of a single operational cycle of an instrument, such as: single large images from electron microscopes, video images from cardio-angiography, sets of related images from MRI procedures and images and numerical from a particle accelerator experiment. The source of such data objects, e.g. centralized health care facilities or large scientific instruments is often remote from the users of the data and from available large-scale storage and computation systems."
"Our Large Data-object Architecture utilizes a high-speed wide-area ATM network between the object sources and a multi-level distributed storage system (DPSS). As the data is being stored, a cataloguing system (ImgLib) automatically creates and stores condensed versions of the data, textual metadata and pointers to the original data. The catalogue system provides a Web based graphical



Akenti Application: Monitoring

interface to the data. The user is able to view the low-resolution data with a standard internet connection and Web browser, or if high-resolution is required can use a high-speed connection and special application programs to view the high-resolution original data."
See <http://www-itg.lbl.gov/WALDO>

